REMARKS/ARGUMENTS

The present application provides a method for creating, storing and reading a new certificate type for certification of keys. In the new certificate type, several certificates, containing redundant data fields, are collated to form one certificate and repetition of redundant information on the certificates is eliminated by use of a group or basic certificate. The group certificate is used where several keys are to be issued at the same time for the same user by the same certification authority. By means of the group certificate, repetition of all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate. This substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners. A particular embodiment of the new certificate types are the basic and supplementary certificate combinations. This form of certification is used where certificates are issued at different times for the same user by the same certification body. The memory requirement is consequently somewhat more than for group certificates, but greater flexibility is gained in use of the keys.

Claim Rejections Under 35 USC 103

A. Claims 1 to 12 were rejected under 35 USC 103(a) as being unpatentable over VeriSign "Certificate Practice Statement", version 1.2, in view of Sutter, U.S. patent #5,924,094, Stallings "Cryptography and Network Security", 2nd Edition, and Karlton "Proposal to Add Attribute Certificates to TLS 3.1".

Applicant's attorney found nothing in the recited combination that teaches combining redundant information for several keys into one group certificate and then issuing supplementary certificates for each of the several keys. With respect to supplementary certificates, the Examiner points out that VeriSign does not teach the use of a supplementary certificates for the issuance of additional keys and relies on the teachings of the Sutter patent and the Karlton reference to provide the missing teaching. However, the subject matter cited in column 49, lines 35 to 39, in the Sutter patent does not mention issuance of supplementary certificates and Karlton clearly states that what is described as an "attribute cert" shall have no associated key pair and cannot be used to establish identity. Therefore, the Karlton teaching specifically excludes use of its attribute cert for applicant's purposes. Accordingly, there not only is a lack of teaching applicant's invention in the proposed combination of Verisign, Sutter and Karlton, but a specific exclusion of any such teaching of the combination for the purposes proposed by applicant in view of Karlton's express statements about configuration and limitation and use of attribute certs. Without the issuance of further keys in applicant's supplementary certificates, the advantages in accordance with the applicant's invention cannot be obtained.

As for group certificates, the Examiner points out that VeriSign does not disclose a certificate designed to carry a plurality of keys in a single group and discusses the Sutter patent in this connection. However, the Sutter patent citation in column 49 does not mention how a certificate for multiple keys is to be configured to cover multiple keys. Therefore there is no teaching in the combination for a group certificate designed to carry multiple keys, as described in the present application.

In addition to the failure of the references to disclose a proper combination of patents to meet the applicant's disclosed invention, the Examiner fails to provide evidence of any suggestions in the references or otherwise (as the time of applicant's invention) to combine and modify the references as suggested by the Examiner. The reasons that the Examiner gives for it being obvious to make the combinations the Examiner proposes essentially breaks down to the need for applicant's invention. That is, it appears that what the Examiner is saying is that in view of this need, those skilled in the art would go through the numerous references in the field, pick out the same four the Examiner has chosen, then modify them just as the Examiner has done and then combine them so as to meet every detail in every one of the 25 claims of the application. This is an unlikely scenario. It appears that what the Examiner has done in his rejection is use hindsight of applicant's disclosure to select certain, otherwise unconnected, references out of a multiplicity of such references and then piece them together and modify them using the applicant's disclosure as an instruction manual and the claims in the application as templates to piece together the teachings of these modified references. The arguments presented by the Examiner for nonpatentability are more applicable to the unobviousness of the applicant's invention since even with all the advantages attributed by the Examiner to the applicant's invention still requires the combination of multiple references in a manner not taught in any of the references.

B. Claims 13 to 18 were rejected under 35 USC 103(a) in view of the combination cited in A further in view of the Deo, U.S. patent #5,721,781.

The addition of the Deo patent to the combination cited in A does not change the failure of the combination cited by the Examiner in A to teach applicant's

invention. Further, the cited sections of Deo do not specifically teach storing and retrieving basic and supplementary certificates in a nonvolatile memory of a chip card. Claim 17, cited in this section, is not limited to a chip card.

C. Claims 19 to 25 were rejected over the prior art cited against claims 1 to 7 in A further in view of "JAVA XZ509 Certificates and Certificate Revocation Lists." The arguments presented in A with respect to claims 1 to 7 apply equally well to the Examiner's position with respect to rejection of claims 19 to 25 in B and C.

The Claims

The claims in the application are all allowable for the reasons given above. Independent claims 1, 8, 10, 15 and 19 all recite basic, group and supplementary certificates or a combination of those certificates in which redundant data elements are listed only once in the basic or group certificate and not repeated in any supplementary certificates. For instance:

Claim 1 calls for a method requiring creation of both a basic certificate and a supplementary certificate for one key and then using the basic certificate in supplementary certificates for keys that share redundant information with the basic certificate. Redundant information is recited as being in the basic certificate and not repeated in the supplementary certificate.

Claim 8 calls for generation of a single group certificate for several keys with all data elements necessary for all keys and key pairs generated in the single group

certificate that contains only a single recitation of data elements redundant to all the keys.

Claim 10 calls for a basic certificate and a subsequently generated supplementary certificate with one of the keys of a generated key pair inserted into the supplementary certificate.

Claim 15 contains a recitation of the sequence of steps to be followed to determine if a chip card contains a relevant key to sign a message.

Claim 19 recites a computer program product containing a basic certificate and at least one supplementary certificate and using the basic certificate with future keys that share the redundant information with the basic certificate by issuing an additional supplementary certificate with a key from a new key pair.

Dependent claims further distinguish over the prior art in that they recite further steps or structure not found in the prior art. For instance:

Claims 2, 3, 4, 7, 9, 11, 20, 21, 23 and 25 recite data elements in basic group or supplementary certificates recited in one or the other of the independent claims. Since there is no supplementary or basic certificates defined by the prior art, these combinations are not taught by the prior art.

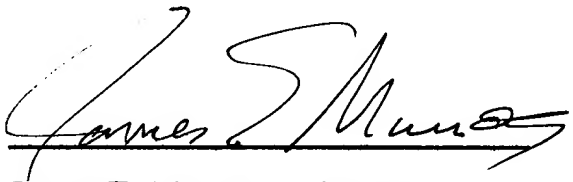
Claims 4, 6, 17, 22 and 24 relate to steps to be taken if one or more keys to be certified at one time.

Claims 13, 14 and 18 further distinguish in that they call for the basic and supplementary certificates to be stored in the nonvolatile memory of a chip card.

As for the Examiner's comments about the organization of certificates not meeting the patentability requirements of an inventive step, applicant's attorney would like to know the statutory basis of this opinion that removes such subject matter from the purview of the patent law.

For the above reasons, the application is in condition for allowance and it is therefore respectfully requested that it be reconsidered, allowed to passed to issue.

Respectfully submitted,



James E. Murray - Attorney

Reg. No.: 20,915

Telephone No.: (845) 462-4763